Information Assurance (Overarching)

Security Classification	**OFFICIAL**
Disclosable under Freedom of Information Act 2000	Yes

POLICY	
REFERENCE NUMBER	**WMP008**
Version	**1.5**

POLICY OWNERSHIP	
DIRECTORATE	CHIEF OFFICERS
BUSINESS AREA	AUDIT, RISK AND COMPLIANCE and DIGITAL SERVICES

INITIAL IMPLEMENTATION DATE	**November 2019**
LATEST REVIEW DATE	**December 2024**
NEXT REVIEW DATE:	**December 2029**
RISK RATING	**MEDIUM**
EQUALITY ANALYSIS	**LOW**

Handling Instructions
This document must be handled and stored according to the Government Security Classifications guidance. Neither the document nor any of its contents may be disseminated further without the permission of the Information Asset Owner.

Document view should be changed to suit individual needs – click Design, Page Colour, Choose page background colour.

1.0 POLICY OUTLINE

Information is an asset which is fundamental to the efficient and effective delivery of policing services. Information comes in many forms, for example, operational data, policy and procedural documents, emails, minutes, statistics, personal data etc. and is held in a variety of manual (hard copy) and electronic formats. West Mercia Police use information daily as we work to deliver our strategic objectives, and deliver efficient, effective, safe and secure services.

To maximise the benefit of information we need to recognise its value, manage it effectively and ensure that it is adequately protected. Information Assurance (IA) relates to the assessment and management of risk relating to the use, processing, storage and transmission of information, and the systems and processes involved in information processing. It encompasses the technical, physical, procedural and personnel controls that address risks to information within an organisation.

This policy sets out the steps that West Mercia Police will take to assure its information and the systems and infrastructure that support it; by protecting its integrity, availability, authenticity and confidentiality. The policy applies to all West Mercia staff, including officers and police staff, working for or on behalf of West Mercia Police and the Offices of the Police and Crime Commissioners for West Mercia staff, volunteers, third party agencies contractors and processors, including personnel on honorary contract, who manage or process information, in any form, on behalf of West Mercia Police.

This policy supports the principals of the statutory guidance, issued by the College of Policing, Accredited Professional Practice (APP) – Information Management and the principles detailed in all sections, particularly Information Assurance (IA). It is supported by a number of procedures relating to various aspects of information management to ensure that information is managed legally, securely, effectively and efficiently.

2.0 PURPOSE OF POLICY

The purpose of this policy is to embed information assurance as a core business activity and to ensure that it is considered in the day to day management and processing of information. The policy and its associated procedures aim to:

- Recognise the value of information as an asset and ensure that appropriate accountability and controls are in place to protect it
- Protect the confidentiality, integrity and availability of information assets, whether electronic, paper based or in any other format
- Ensure that an appropriate governance framework is in place for information management and addressing information risk
- Ensure that officers, staff, volunteers, third parties and contractors are trained and aware of their responsibilities for managing information

- Ensure that technology and information systems operate securely and meet His Majesty's Government (HMG) accreditation and information assurance standards, including the National Police Community Security Policy (CSP), Security Assurance for Policing (SyAP) and National Codes of Connection (CoCo)

- Ensure that West Mercia Police meet statutory, legal, national and best practices standards for information management

3.0 IMPLICATIONS of the POLICY

The effective operation of this information assurance policy and associated procedures will support the delivery of effective policing services, enable better business planning, reduce cost and protect people from harm by ensuring that information is secure, accurate and available to the right people at the right time.

This policy and associated procedures support compliance with legal, national and best practice standards including;

- Freedom of Information Act 2000
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Equality Act 2010
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Government Security Classifications June 2023
- HMG Security Policy Framework
- National Police Community Security Policy
- College of Policing Authorised Professional Practice (APP) – Information Management and its principles including Information Assurance (IA), Management of Police Information (MoPI)
- International Organisation for Standardisation (ISO) 27001:2013 Information Security Management
- British Standard (BS) 10008:2008 Evidential weight and legal admissibility of electronic information.
- Security Assurance for Policing (SyAP)
- National Institute of Standards and Technology Cyber Security Framework (NIST CSF) 1.2

Failure to comply with the policy could result in impact on:

- Legal compliance
    - Breach of Data Protection Act 2018 or other applicable law
- Financial
    - GDPR fines of up to 20 million euros (circa 16 million pounds) or 4% of turnover for personal data breaches
    - Cost of managing, investigating and recovering from incidents
- Personal
    - Risk of harm to individuals if information is subject to unauthorised disclosure, inaccurate, or unavailable

- Reputational
  - Loss of reputation and public confidence in the police
- Operational
  - Inability to deliver services if information is not available to the right people and/ or cannot be relied upon as accurate

- Government/ Policing Standards
  - Failure to meet HMG standards for connection to Public Service Network (PSN), its replacement Law Enforcement Data Service (LEDS) and National Systems (which may result in increased costs and operational impact)

4.0 POLICY STATEMENT

Good information assurance requires clear and effective management and accountability structures, assurance processes, documented policies and procedures, trained staff and adequate resources.

4.1 Information Assurance Management and Governance

West Mercia Police must have clear lines of accountability for information assurance, with key roles in place based on the Cabinet Office Information Risk Framework, and information assurance monitored and managed through the appropriate governance groups.

Appendix A outlines the key roles and responsibilities for information assurance.

Appendix B outlines the governance groups in place for information assurance

4.2 Risk Management

Processes must be in place for managing risk that reflect business objectives to support good risk management. This includes assessments to identify potential threats, vulnerabilities and appropriate controls to reduce risks to people, information and infrastructure, with assurance processes to ensure that mitigations are effective.

4.3 Data Flow Mapping

Once an Information Asset has been identified, along with the risk relating to this, a data flow map will need to be created.

The links between the Information Asset Register (IAR) and the data flow mapping process will then identify any risks, which means that we can ensure assets are identified and protected. This means we can reduce the potential for errors, standardise our data and make it easier for us to understand.

To ensure we are complying with GDPR (General Data Protection Regulations) and RoPA (Record of Processing Activities) we need to make sure we are capturing the type of data we are collecting, the sensitivity and source of the data, the purpose for which it is being collected and what it is being used for. We also need to capture the storage period, locations, conditions, transfer destinations and data transfer protocols. This approach will ensure that we are properly protecting our personal data in our article 30 documentation and will help us to create a complete and comprehensive record of processing activities.

See Data Flow Mapping Guidance WMP202

4.4 Information Risk Screening

The Information Risk Screening process enables information risks to be identified and managed at the initial stage of a project or activity. These could be risks relating to the information itself (in terms of confidentiality, integrity, and/ or availability, classification, sensitivity and personally identifiable), technology and services, physical security (including third parties involved in the activities) or processes.

Project Teams and Business Leads are responsible for ensuring an Information Risk Screening Form (IRSF) is submitted to the Information Security function so advice can be given on what further assurances and/ or resources may be required to ensure that the project or activity is delivered securely, safely, and in compliance with national Information Assurance and Data Protection standards and legislation, including the UK Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

4.5 Information

Mechanisms and processes must be in place to ensure assets are properly classified and appropriately protected, and there is confidence that systems and services can protect the information that they carry.

4.6 Technology and Services

Procedures must be in place to protect against, detect and correct malicious behaviour. Critical technology and services will be resilient to cyber incidents and have the means to recover from these.

4.7 Personnel Security

Processes must be in place for pre-employment vetting checks and ongoing security management of people with access to information, with regular monitoring and assurance, to mitigate insider risk.

4.8 Physical security

Processes and plans must in place to determine and implement appropriate physical security controls for information assets based on their criticality and sensitivity.

4.9 Information Security Incident Procedures

Processes must be in place for reporting, managing and resolving any security incidents. This includes ensuring organisational learning from incidents. Business continuity arrangements must ensure resilience, and ensure quick and effective recovery from incidents.

4.10 Cloud Hosting Services

West Mercia Police owns and utilises a range of information assets and systems to provide policing services; such information assets can be stored either internal or external to the force ICT network. On occasion that can involve the use of cloud service providers to host data and/ or information systems off-site and external to the force ICT network.

Project Teams are responsible for the early engagement of the Information Security function in the system implementation or change projects where there is a confirmed or potential requirement for the use of cloud hosting services. The force recognises the need to ensure that robust assessment is undertaken to ensure that appropriate controls are in place, with the outcome of the security and technical risk assessments fully auditable and signed off at the appropriate level.

4.11 Training and Awareness

All officers, staff, volunteers, third parties and contractors must be aware of their own personal responsibilities for managing information, and undertake the appropriate training in line with National Police Chiefs' Council (NPCC) requirements.

This includes the completion of the relevant NCALT Managing Information courses and additional specialist training for specific job roles:

	Managing Information- Relevant module (Operational/ Non-Operational)	**Protecting Information- Level Two**	**Protecting Information- Level Three**	**Data Protection Foundation Level**
All officers, staff, contractors, volunteers	Mandatory	Not Required	Not Required	Mandatory
Senior Information Risk Owner (SIRO)	Mandatory	Mandatory	Mandatory	Mandatory
Senior Information Asset Owner/Information Asset Owners	Mandatory	Mandatory	Mandatory	Mandatory
Information Asset Nominated Officers	Mandatory	Mandatory	Not Required	Mandatory
Data Protection Officer	Mandatory	Mandatory	Mandatory	Mandatory
Information Security Manager/ Officer	Mandatory	Mandatory	Mandatory	Mandatory

'Any individual who fails to complete mandatory training and pass the associated competency tests should be given time to re-sit the training and pass the test. The individuals line manager / supervisor will decide whether the individual requires additional training prior to re-sitting the test. Any individual who fails a second time should be given one-to-one instruction under arrangements made by their line manager / supervisor.

Consistent and repeated failure may result in the individual being denied access to the force network and all systems until the required standard is attained. In this event the individual's line manager / supervisor should assess the risk of leaving the individual in any role with unsupervised access to personal data and take action accordingly'.

5.0 PROCEDURE

This is the overarching policy for information assurance. This, and its supporting procedures are aligned to HMG Security Policy Framework and recognised standards that Government and Public Sector bodies adhere to for information assurance. Procedures that are currently in place to support this policy include:

- **Personnel Security Procedure (WMP008a)**
  This sets out the requirements in relation to the vetting of all Force personnel - and those of third party suppliers, contractors and Partner Agencies - who have access to the Forces' information assets or the equipment on which they are processed.

- **Clear Desk and Clear Screen Procedure (WMP008b)**
  This informs all members of the Force and OPCC and occupants of police premises - and those that police share with others - how information assets should be securely stored when not in use. It also advises how unauthorised access to displayed information assets should be prevented.

- **Information Classification Procedure (WMP008f)**
  This sets out how the Force will implement their chosen valuation and Marking scheme for their information assets - the Government Security Classification (GSC) scheme.

- **Account Management Procedure (WMP008j)**
  This sets out the requirements for the secure management of such accounts and their access credentials (e.g. passcodes or Smartcards) once issued. This includes the deletion and disabling of accounts and/or access credentials.

- **Password Procedure (WMP008l)**
  This sets out to highlight that information is a valuable asset and consequently needs it to be suitably protected. Protecting information is not only an organisational responsibility; it is also a responsibility which all staff, including partner agencies, delivery partners, and third party suppliers, must take seriously.

- **Information Security Incident Management Procedure (WMP008e)**
  This sets out the process for the reporting, and subsequent investigation, of deliberate, accidental or potential security incidents involving the Force and OPCC information assets and premises (whether or not shared with others).

- **Data Sanitisation and Secure Disposal Procedure (WMP008k)**
  This describes how the Force and OPCC ensure that redundant information assets and any equipment on which they have been processed, should be disposed of, to prevent such data being accessed inappropriately.

- **Protective Monitoring Procedure (WMP008h)**
  This describes the process by which ICT system activity is logged in order to provide an audit trail of security events of interest and when and how such data is subsequently used.

- **Off-Site Security of Police Information and Equipment Procedure (WMP008i)**
  This sets out the security countermeasures to reduce the risks of compromise of

the Forces' information, and information-processing, assets to an acceptable level when they are not on secured Police Premises.

- **Data Protection Policy (WMP017)**
  This sets out the requirements of the Data Protection Act 2018 and provides West Mercia Police employees, including special constables, volunteers and contractors, with appropriate guidance to assist them in their day to day activities in support of the policing purpose.

- **Data Protection Impact Assessment Procedure (WMP069)**
  This sets out the process for how the force will conduct Data Protection Impact Assessments (DPIAs) as required by the Data Protection Act 2018 and the General Data Protection Regulation (GPDR).

6.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the chart below:

Date	Author / Reviewer	Amendment(s) & Rationale	Date of Approval / Adoption
Dec 2018	A Baylis	Previously Approved at JNCC	11/12/2018
Nov 2019	E Peberdy	Reviewed – Updated to West Mercia Policy. Minor change to training table SIAO/SIO Level 2 now mandatory, v1.0	12/11/2019
Feb 2021	M Snow	Updated to include cloud hosting services requirements. Changes made to training table Level 2 now recommended for all officers, staff, contractors and volunteers, and ISM/ ISO and mandatory for SIRO, IANO and DPO. Level 3 now mandatory for SIAO/ IAO/ ISM/ ISO. Managing Information and Data Protection Foundation now mandatory for ISM/ ISO. v1.1	23/02 2021
Mar 2021	M Snow	Following ICO audit review, Updated to include reference to Information Risk Screening 4.3 and the DP policy and DPIA procedure added as links to overarching policy. v1.2	18/03/2021
Oct 2021	M Snow/ Dan Archer	Deletion of Passcode Management procedure, replaced with Password procedure v1.3	Exec Board outside of JNCC 06/05/2021
Dec 2022	D Jeynes	Addition of Data Flow paragraph at 4.3 v 1.4	23/12/2022
Nov 2024	N Lowe	Minor updates to legislation versions and addition of SyAP, and cosmetic changes such as the new logo	18/11/2024

7.0 CONSULTATION

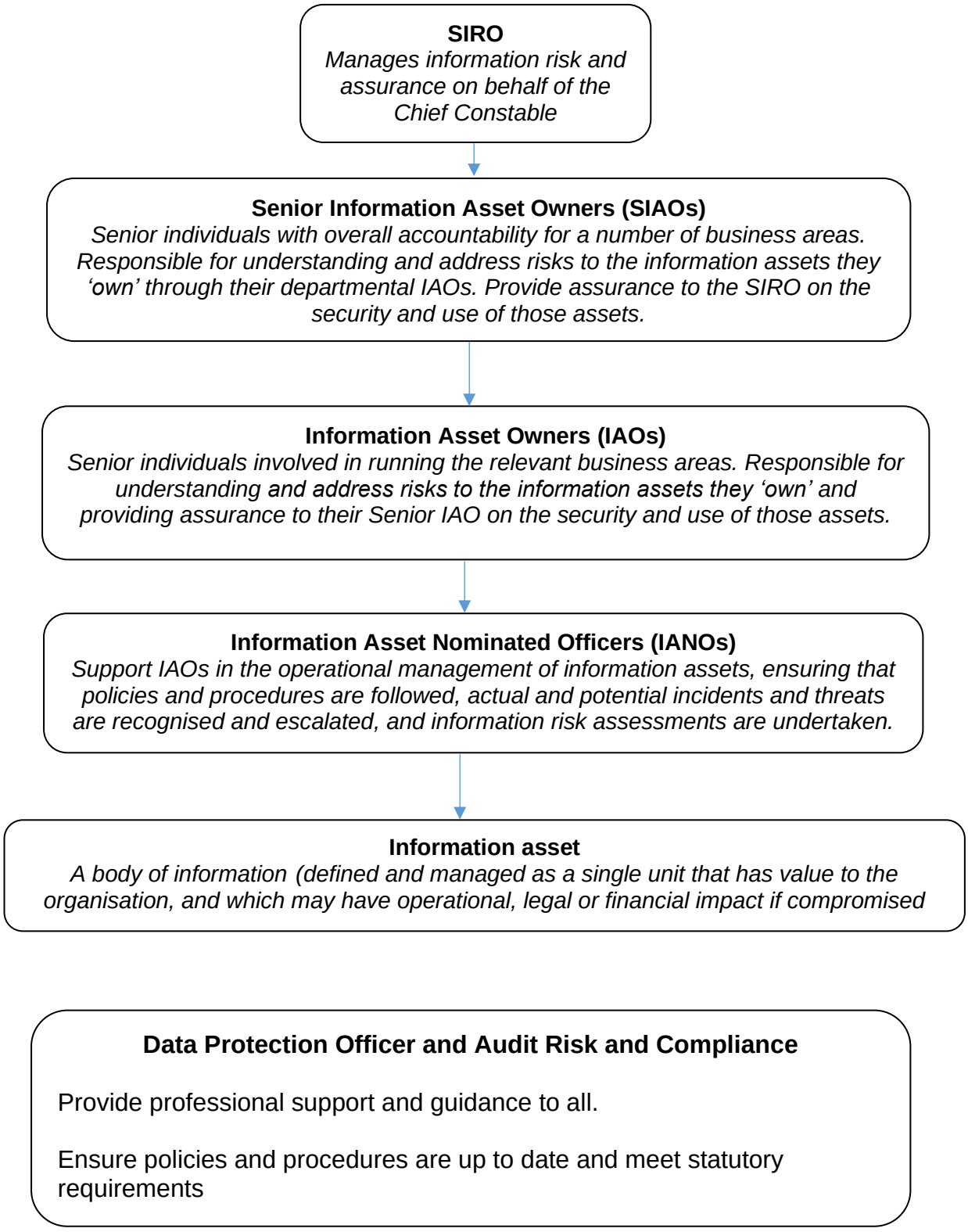
Business Lead Consulted	***Date Consulted***
Elaine Peberdy	December 2022
Elaine Peberdy	December 2024

Consultation with: ARC management, ICT Senior Leads, Strategic Risk, Professional Standards (including Vetting), Training and relevant Senior Management and members of the Critical Friends group (2021)

8.0 ASSESSMENT AND ANALYSIS

The Equality Assessment (EA), Health & Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.

APPENDIX A: Structure for Information Assurance



APPENDIX B: Governance Arrangements for Information Assurance